October 12, 2004

Information Technology

Reporting of DoD Capital Investments for Technology in Support of the FY 2005 Budget Submission

(D-2005-002)

Department of Defense
Office of the Inspector General

Quality *Integrity* *Accountability*

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **12 OCT 2004**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE
Reporting of DoD Capital Investments for Technology in Support of the FY 2005 Budget Submission

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Office of the Inspector General Department of Defense 400 Army Navy Drive Arlington, VA 22202-4704

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**18**	

Additional Copies

To obtain additional copies of this report, visit the Web site of the Inspector General of the Department of Defense at http://www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit, Audit Followup and Technical Support at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact Audit Followup and Technical Support at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

ODIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General of the Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

DEPARTMENT OF DEFENSE
hotline

To report fraud, waste, mismanagement, and abuse of authority.

Send written complaints to: Defense Hotline, The Pentagon, Washington, DC 20301-1900
Phone: 800.424.9098 e-mail: hotline@dodig.osd.mil www.dodig.osd.mil/hotline

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

October 12, 2004

MEMORANDUM FOR ASSISTANT SECRETARY DEFENSE (NETWORKS AND INFORMATION INTEGRATION) / DOD CHIEF INFORMATION OFFICER

SUBJECT: Reporting of DoD Capital Investments for Technology in Support of the FY 2005 Budget Submission (Report No. D-2005-002)

We provided a draft of this report on September 28, 2004. No written response to this report was required and none was received. Therefore, we are publishing this report in final form.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Ms. Kathryn M. Truex at (703) 604 8966 (DSN 664-8966) or Mr. Robert L. Shaffer at (703) 604-9043 (DSN 664-9043). See Appendix B for the report distribution. The team members are listed inside the back cover.

Mary L. Ugone

Mary L. Ugone
Assistant Inspector General for
Acquisition and Technology Management

Office of the Inspector General of the Department of Defense

Report No. D-2005-002 **October 12, 2004**
(Project No. D2004AL-0148)

Reporting of DoD Capital Investments for Technology in Support of the FY 2005 Budget Submission

Executive Summary

Who Should Read This Report and Why? DoD managers preparing and certifying capital investment justifications for information technology should read this report to improve the quality of data being submitted by the Assistant Secretary of Defense (Networks and Information Integration) to the Office of Management and Budget and Congress.

Background. Information technology is a President's Management Agenda priority for expanding electronic government. In addition, Congress has challenged the quality of DoD information technology management because information technology documents and associated budget data that DoD provided were inaccurate, misleading, or incomplete. In FY 2005, DoD submitted a budget request of $28.7 billion for information technology.

Results. DoD Components did not adequately report information technology investments to the Office of Management and Budget in support of the DoD Budget Request for FY 2005 because Component Chief Information Officers and Chief Financial Officers did not always include required information in submitted reports. Specifically, 76 of 174 (44 percent) Capital Investment Reports submitted to the Office of Management and Budget in standard formats did not completely respond to one or more required data elements addressing security funding, certification and accreditation, and training and security plans. As a result, the quality of DoD security information reported to the Office of Management and Budget had limited value and did not demonstrate, in accordance with Office of Management and Budget and DoD guidance, that DoD was effectively managing its proposed information technology investment for FY 2005.

In response to prior audit reports by the Government Accountability Office and the Office of the Inspector General of the Department of Defense, the Assistant Secretary of Defense (Networks and Information Integration) / DoD Chief Information Officer either concurred or partially concurred with the recommendations and took actions that should improve the quality of Capital Investment Reports submitted to the Office of Management and Budget for FY 2006. Therefore, we made no recommendations.

Table of Contents

Background

DoD Components use information technology in a wide variety of mission functions including finance, personnel management, computing and communication infrastructure, logistics, intelligence, and command and control. Information technology consists of any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The President's Management Agenda for expanding electronic government identified effective planning for information technology investments as a priority. Improving information technology security is one of the Office of Management and Budget's highest priorities in information technology management. In addition, Congress has challenged the quality of DoD information technology management because information technology documents and associated budget data that DoD provided were inaccurate, misleading, or incomplete. The Assistant Secretary of Defense (Networks and Information Integration), as the Chief Information Officer, is the principal staff assistant to the Secretary of Defense for DoD information technology.

Public Law 107-347, Title III, "Federal Information Security Management Act of 2002," December 17, 2002, requires agencies to address the adequacy and effectiveness of information security policies and practices in plans and reports relating to annual agency budgets.

Public Law 104-106, "National Defense Authorization Act for Fiscal Year 1996," Division E, Information Technology Management Reform, February 10, 1996, commonly called the "Clinger-Cohen Act," requires effective and efficient capital planning processes for selecting, managing, and evaluating the results of all major investments in information technology. The Act requires that executive agencies:

- Establish goals for improving the efficiency and effectiveness of agency operations through the effective use of information technology,
- Prepare an annual report, to be included in the executive agency's budget submission to Congress, on the progress in achieving the goals,
- Prescribe performance measurements for information technology and measure how well information technology supports agency programs,
- Measure quantitatively agency process performance for cost, speed, productivity, and quality against comparable processes and organizations in the private and public sectors where they exist,
- Analyze the missions of the executive agency and, based on the analysis, revise the executive agency's mission-related processes and administrative processes as appropriate before making significant investments in information technology, and
- Ensure that information security policies, procedures, and practices of the executive agency are adequate.

DoD uses the Information Technology Management Application database to plan, coordinate, and disseminate the DoD information technology budget that the Office of Management and Budget and Congress require. The information technology budget for FY 2005 totaled $28.7 billion and consisted of 1,176 different initiatives. DoD classified 172 of the initiatives as major investments, which accounted for $13.1 billion (46 percent of the information technology budget). The remaining 1,004 initiatives were minor investments and totaled $15.6 billion.

Components must submit an Exhibit 300, "Capital Investment Report," for all major information technology investments. Major information technology investments:

- require special management attention because of their importance to an agency's mission;
- were included in the FY 2004 submission and are ongoing;
- are for financial management and more than $500,000;
- are directly tied to the top two layers of the Federal Enterprise Architecture;
- have significant program or policy implications;
- have high executive visibility;
- are defined as major investments by the agency's capital planning and investment control process.

The Capital Investment Report is used by DoD management and the Office of Management and Budget to show that the Component has employed the disciplines of good project management, presented a strong business case for the investment, and defined the proposed costs, schedule, and performance goals for the investment if funding approval is obtained. When submitted, the Capital Investment Report should be complete and accurate and provide all the information that the Office of Management and Budget requires. In September 2003, DoD submitted 174 Capital Investment Reports for the FY 2005 budget request to the Office of Management and Budget.

Objectives

The overall audit objective was to verify and validate whether the Services and DoD Components are adequately reporting information technology investments to the Office of Management and Budget. Specifically, the audit determined whether DoD Capital Investment Reports that were submitted in September 2003 for the Office of Management and Budget FY2005 reporting requirements demonstrated that DoD is managing its information technology investments in accordance with Office of Management and Budget and DoD guidance.

Completeness of DoD Capital Investment Reports

DoD Components did not adequately report information technology investments to the Office of Management and Budget in support of the DoD Budget Request for FY 2005 because Component Chief Information Officers and Chief Financial Officers did not always include the required information in the reports that they submitted. Specifically, 76 of the 174 (44 percent) Capital Investment Reports submitted to the Office of Management and Budget in September 2003 did not completely respond to one or more required data elements in the Security and Privacy section. As a result, the quality of DoD information reported on security to the Office of Management and Budget had limited value and did not demonstrate, in accordance with Office of Management and Budget and DoD guidance, that DoD was effectively managing its proposed $28.7 billion information technology investment for FY 2005.

Criteria

Office of Management and Budget Circular A-11. Circular A-11, "Preparation, Submission, and Execution of the Budget," Part 7, Section 300, "Planning, Budgeting, Acquisition, and Management of Capital Assets," July 2003, implements the Clinger-Cohen Act and establishes policy and procedures for planning, budgeting, acquiring, and managing Federal capital assets. Agencies are required to demonstrate to the Office of Management and Budget in semi-annual reports that major information technology investments are directly connected to agencies' strategic plans and provide a positive return on investment, sound acquisition planning, comprehensive risk mitigation and management planning, realistic cost and schedule goals, and measurable performance benefits. For the DoD FY 2005 budget request, the Assistant Secretary of Defense (Networks and Information Integration) / DoD Chief Information Officer forwarded 174 Capital Investment Reports to the Office of Management and Budget. The Capital Investment Report is the primary means of justifying and managing information technology investments.

DoD Financial Management Regulation. The DoD Financial Management Regulation, 7000.14-R, Volume 2B, Chapter 18, "Information Technology Resources and National Security Systems," June 2002, requires all DoD Components that have any resource obligations for information technology or national security systems to prepare Capital Investment Reports, which are mandated by Office of Management and Budget Circular A-11. The regulation requires Component Chief Information Officers and Chief Financial Officers to jointly certify that the Capital Investment Reports submitted are complete, accurate, and consistent with the Clinger-Cohen Act, the Paperwork Reduction Act, and other applicable acts and requirements.

Capital Investment Reports to Office of Management and Budget

The Information Technology Capital Investment Reports submitted for the FY 2005 DoD budget request did not demonstrate that DoD was effectively and efficiently managing information technology resources in accordance with the Office of Management and Budget Circular A-11, July 2003. Our analysis showed that 76 of the 174 (44 percent) of Capital Investment Reports that DoD submitted to the Office of Management and Budget contained incomplete information or did not provide the information that was required by Circular A-11 for one or more of the data elements in the Security and Privacy section. Incomplete information was submitted in the data elements for security funding, certification and accreditation, incident handling and reporting, security plans, contractor security, security testing, security training, and the protection of systems accessible to the public. In addition, we also reviewed Component responses on whether they reviewed their investments during the FY 2003 Federal Information Security Management Act reporting process.

Security Funding. Circular A-11 requires Components to describe how security is provided and funded and report the total dollars allocated for information technology security for all investments in FY 2005. Fifty-three of the 174 submissions (30 percent) were incomplete. Thirty-four Components reported security funding for FY 2004 rather than FY 2005. An additional 12 Components reported that security funding for FY 2005 was unavailable. We were unable to determine the amount of security funding for seven investments based on the information given. Table 1 summarizes the incomplete information on security funding that Components submitted.

Table 1. Incomplete Submissions for Security Funding by Component

Component	Number of Incomplete Submissions	Percent
Army	24 of 44	55
Navy	7 of 36	19
Air Force	2 of 24	8
Defense agencies	20 of 70	28
Total	**53 of 174**	**30**

Certification and Accreditation. Circular A-11 reporting requirements require Components to verify full certification and accreditation for investments, specify the methodology used, and provide the date of the last certification and accreditation review. Full certification and accreditation refers to investments with authority to operate and excludes investments with interim authority to operate. All information technology investments must be fully certified and accredited before becoming operational. Anything short of full certification and accreditation indicates that identified information technology security weaknesses remain. These weaknesses must be corrected before adequate funding for the investment can be justified. In 61 of the 174 submissions (35 percent), the Capital Investment Reports did not support full certification and accreditation. Components included investments with interim authority to operate, investments where the certification and accreditation was in process, or the status of certification and accreditation was unclear.

Office of Management and Budget Memorandum 03-19, “Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on IT [Information Technology] Security Reporting,” August 6, 2003, requires Federal agencies to prepare and submit Plan of Action and Milestones documents for all programs and systems with information technology security weaknesses. However, only 22 of the 61 investments had a Plan of Action and Milestones document. Twelve additional Capital Investment Reports did not contain the certification and accreditation methodology used or the date of the last certification and accreditation review. One Component reported that the question on certification and accreditation was not applicable because the investment, “Common Operating Environment,” was not a system, it is a collection of software components that are integrated into mission applications and command and control systems. The Component stated that systems that use the software components of the “Common Operating Environment” are taken through the certification and accreditation process by the organization owning the system. We believe that the question does apply to the Component. DoD Instruction 5200.40, “DoD Information Technology Security Certification and Accreditation Process,” December 30, 1997 paragraph E3.4.3.3.2, clearly describes the software design certification task and states that the task may include a detailed analysis of software specifications and software design documentation. Table 2 summarizes the 73 Capital Investment Reports, by Component, of submissions that were incomplete or did not support full certification and accreditation.

Table 2. Inadequate Certification and Accreditation Submissions by Component

Component	Number of Incomplete Submissions	Percent
Army	22 of 44	50
Navy	20 of 36	56
Air Force	8 of 24	33
Defense agencies	23 of 70	33
Total	**73 of 174**	**42**

Incident Handling and Reporting. Circular A-11 requires Components to report on how incident-handling capability has been incorporated into the system or investment and to include a summary of intrusion detection monitoring and audit log reviews. Circular A-11 also requires Components to report incidents to the Department of Homeland Security’s Federal Computer Incident Response Center. Thirteen of the 174 (7 percent) Capital Investment Reports did not address all of the required elements, including intrusion detection monitoring and audit log reviews. In two submissions, the Component reported that the investment was a new start and that the security requirements were being developed.

Security Plans. Circular A-11 requires Components to report whether the investments have an updated security plan and provide the date of the plan. A reference to security plans or other documents is not an acceptable response. Fourteen of the 174 (8 percent) Capital Investment Reports did not provide the date of the security plan, did not indicate that an updated security plan was available, or stated that the requirement was not applicable. Reasons provided for the security plan not being applicable included:

- The contract has not been awarded, but all required security issues would be addressed and the re-hosted system would contain all the security features that are currently available in the system.

- The program did not process any information or data; it provided an infrastructure to house computers and radios used in Army command posts.

We do not consider those answers responsive to the question on security plans. Circular A-11 clearly states that all information technology investments must have up-to-date security plans.

Contractor Security. Circular A-11 requires Components to report whether the contractor operated the system on site or at a contractor facility and whether the contract includes specific security requirements required by law and policy. Circular A-11 also requires Components to describe how contractor security procedures are monitored, verified, and validated. Ten of the 174 (6 percent) Capital Investment Reports did not completely address all the elements for this area. Component responses stated that the investment was not a system, that the requirement did not apply, or that new start authority was pending. In other submissions, the responses were too general to be useful. Examples of the complete answers that were too general were:

- "Any contractors undergo background evaluations."
- "By sites security administrator."
- "Yes, security investigation of contractors is required, bound by same access rules as Government employees."

Security Testing. Circular A-11 requires Components to report on whether management, operational, and technical security controls have been tested for effectiveness. Circular A-11 also requires the Components to provide the date of the most recent tests. Eleven of the 174 (6 percent) Capital Investment Reports did not contain the required information for this area. Six Components failed to include the date of the most recent tests. Five Components stated that the investment was not a system and did not provide the requested information.

Security Training. Circular A-11 requires Components to provide information on user training in the past year. Five of 174 (3 percent) Capital Investment

Reports did not clearly show that the users were appropriately trained during the past year or that the requirement was not applicable.

Protection of Systems with Public Access. Circular A-11 requires Components to report on how agencies ensure effective use of security controls and authentication tools to protect privacy for systems that promote or permit public access. Three of the 174 (2 percent) Capital Investment Reports stated that this program is pending new start authority, security requirements were being identified within the architecture products, or that the requirement was not applicable.

Federal Information Security Management Act. Circular A-11 requires Components to report whether they reviewed investments as part of the FY 2003 Federal Information Security Management Act reporting process, whether the review indicated any weaknesses, and whether the weaknesses were included in the corrective action plan. Our review of the 174 Capital Investment Reports showed that 83 (48 percent) investments were included as part of the review. Thirteen of the 83 reports indicated weaknesses were found and incorporated into an agency corrective action plan. Office of Management and Budget Memorandum 03-19, "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on IT [Information Technology] Security Reporting," August 6, 2003, requires Federal agencies to prepare and submit Plan of Action and Milestones documents for all programs and systems with any information technology security weakness. However, only 3 of the 13 reports that indicated weaknesses had a Plan of Action and Milestones document. In addition, two of the Capital Investment Reports did not answer the question.

Effect of Inadequate Capital Investment Reports

The quality of DoD information reported on security to the Office of Management and Budget had limited value because it did not demonstrate, in accordance with Office of Management and Budget and DoD guidance, that DoD was effectively managing its $28.7 billion information technology investment for FY 2005. Although Capital Investment Reports are officially submitted to the Office of Management and Budget twice yearly, Components should use them as management tools and update the reports as the information becomes available. Information reported on Capital Investment Reports helps management ensure that spending on capital assets directly supports an agency's mission and will provide a return on investment equal to or better than alternative uses of funding. Submission of incomplete reports jeopardizes appropriate funding and diminishes the overall usefulness of Capital Investment Reports.

Management Actions Taken on Previous Audits and During this Audit

The Congress, the Government Accountability Office (formerly, the General Accounting Office), and the Inspector General of the Department of Defense have questioned the quality, accuracy, and completeness of DoD budget submissions.

However, the Assistant Secretary of Defense (Networks and Information Integration) / DoD Chief Information Officer has taken action that should improve the quality of future Capital Investment Reports submitted to the Office of Management and Budget.

Congressional Interest. In the past, the House Committee on Armed Services has challenged the quality of DoD information technology management. The Committee noted that DoD information technology documents provided to the Committee describing the various information technology initiatives and associated budget data were inaccurate, misleading, or incomplete.

Government Accountability Office. The Government Accountability Office assessed the funding information in the DoD Information Technology Budget Summary to determine the reliability of the DoD FY 2004 budget submission for information technology. Audit Report GAO-04-115, "Improvements Needed in the Reliability of Defense Budget Submissions," December 19, 2003, found that the FY 2004 information technology budget submission contained material inconsistencies, inaccuracies, or omissions that limited its reliability. The report made eight recommendations to improve the reliability of future budget submissions and raise the level of management attention on improving reliability and strengthening the management processes and supporting systems. In response to the report's recommendations, the Assistant Secretary of Defense (Networks and Information Integration) / DoD Chief Information Officer agreed or partially agreed with the recommendations and described actions that his office would take to establish the appropriate controls and systems needed to correct many of the weakness described in the report.

Inspector General of the Department of Defense. The Office of the Inspector General of the Department of Defense assessed the "Reporting of DoD Capital Investments for Information Technology," May 7, 2004 (Report No. D2004-081). The report determined that DoD Capital Investment Reports submitted to the Office of Management and Budget and Congress for information technology assets did not consistently demonstrate that information supporting the budget justifications was directly connected to the DoD strategic plan and would provide a positive return on investment, sound acquisition planning, comprehensive risk mitigation and management planning, realistic cost and schedule goals, and measurable performance benefits. In response to the report's recommendations, the Assistant Secretary of Defense (Networks and Information Integration) / Chief Information Officer revised the DoD Financial Management Regulation to make DoD financial officers more accountable for submitted data. The revised guidance augmented compliance with the Clinger-Cohen Act and Office of Management Budget Circular A-11 requirements.

Status Meetings. The Director of Resources, Assistant Secretary of Defense (Networks and Information Integration) / DoD Chief Information Officer held numerous meetings with officials of the Services and Defense agencies who were responsible for preparing and submitting the FY 2006 DoD information technology Capital Investment Reports and other associated budget data in an effort to clarify the Office of Management and Budget guidance and improve the quality of Capital Investment Reports submitted.

Submission Process Changes. On July 19, 2004, the Assistant Secretary of Defense (Networks and Information Integration) / DoD Chief Information Officer issued policy and guidance for completing and submitting the FY 2006 Capital Investment Reports. Starting with the FY 2006 Exhibit 300 submissions, the Director of Resources, Office of the Assistant Secretary of Defense (Networks and Information Integration) / Chief Information Officer plans to score all submissions using an established self-assessment process. The Director will also inform DoD Components of required revisions before forwarding them to the Office of Management and Budget. When implemented, those actions should further improve the quality of Capital Investment Reports submitted to the Office of Management and Budget.

Conclusion

The quality of security information reported to the Office of Management and Budget for FY 2005 did not consistently demonstrate that Components were effectively managing information technology capital assets. Although reasonable explanations existed for some missing and incomplete data, this rationale could not be applied systemically for the majority of missing or incomplete information responses. Actions taken by the Assistant Secretary of Defense (Networks and Information Integration) / DoD Chief Information Officer in response to audit reports by the Government Accountability Office and the Office of the Inspector General should improve the quality of the Capital Investment Reports submitted to the Office of Management and Budget for FY 2006. Therefore, we are not making any recommendations.

Appendix A. Scope and Methodology

We examined all 174 Capital Investment Reports that DoD submitted to the Office of Management and Budget for the FY 2005 DoD Budget Request. We limited our review to evaluating the responses in the data elements of security funding, certification and accreditation, incident handling and reporting, security plans, contractor security, security testing, security training, and protection of systems accessible to the public. We also reviewed Component responses on whether investments were reviewed during the FY 2003 Federal Information Security Management Act reporting process. We evaluated the reporting process and the completeness of information for each report based on report preparation guidance from Office of Management and Budget Circular A-11, Part 7, "Planning, Budgeting, Acquisition, and Management of Capital Assets," July 2003, and the DoD Financial Management Regulation 7000.14-R, Volume 2B, Chapter 18, "Information Technology Resources and National Security Systems," June 2002. We also reviewed relevant documents addressing report submissions from February 1996 through July 2004.

We attended meeting with officials who were responsible for preparing and submitting DoD information technology Capital Investment Reports and other associated budget data within the Services and Defense agencies to gain an overall understanding of the information technology budget process.

This audit was performed from April 2004 through September 2004 in accordance with generally accepted government auditing standards. The management control program was not an announced audit objective because it was reviewed and reported upon in Inspector General Report Number D-2004-081.

Use of Computer-Processed Data. We did not use computer processed data to perform this audit.

Use of Technical Assistance. We did not use technical assistance to perform this audit.

Government Accountancy Office High-Risk Area. The General Accounting Office has identified several high-risk areas in DoD. This report provides coverage of DoD Information Technology management.

Prior Coverage

GAO Report Number GAO-04-115, "Improvements Needed in the Reliability of Defense Budget Submissions," December 19, 2003

Inspector General Report Number D-2004-081, "Reporting of DoD Capital Investments for Information Technology, May 7, 2004

Appendix B. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)/Chief Financial Officer
Assistant Secretary of Defense (Networks and Information Integration) / DoD Chief Information Officer
Director, Program Analysis and Evaluation

Joint Staff

Director, Joint Staff

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Chief Information Officer, Department of the Army
Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Chief Information Officer, Department of the Navy
Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Chief Information Officer, Department of the Air Force
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency

Non-Defense Federal Organization

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency and Financial Management, Committee on Government Reform
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform

Team Members

The Office of the Deputy Inspector General for Auditing of the Department of Defense, Acquisition and Technology Management prepared this report. Personnel of the Office of the Inspector General of the Department of Defense who contributed to the report are listed below.

Mary L. Ugone
Kathryn M. Truex
Robert L. Shaffer
George A. Leighton
Robert R. Johnson
Jacqueline N. Pugh